UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

TRISTRATA, INC.,
Plaintiff,
v.
MICROSOFT CORPORATION, et al.,
Defendants.

Case No. 11-cv-03797-JST

ORDER CONSTRUING CLAIM TERMS, DENYING MOTION TO STRIKE TECHNOLOGY TUTORIAL, AND GRANTING MOTION TO SUPPLEMENT RECORD ON CLAIM CONSTRUCTION

Before the Court are the parties' competing constructions of several claim terms contained in U.S. Patent Nos. 7,257,706 ("the '706 patent'") and 7,743,249 ("the '249 patent'"), which the Court now construes pursuant to Markman v. Westview Instruments, Inc., 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc), aff'd, 517 U.S. 370 (1996), and Patent Local Rule 4–3. Also before the Court are Defendants' Motion to Strike Portions of TriStrata's Technology Tutorial, ECF No. 100, which the Court will deny, and Plaintiff's Motion to Supplement the Record on Claim Construction, ECF No. 123, which the Court will grant.

I. BACKGROUND

A. Relevant Cryptography Background

The study of securely transmitting information from one party to another is known as cryptography. Cryptographers develop methods and tools for obscuring the contents of a document or communication so that third parties cannot know its contents. One such tool is encryption, the process through which a document, which begins as readable in "plaintext," is converted into "ciphertext," an indecipherable collection of characters. Ciphertext is converted back to plaintext through decryption. Encryption and decryption are accomplished via algorithms — mathematical functions that evaluate plaintext or ciphertext alongside a "key" in order to translate from one to the other. Encryption and decryption keys are typically alphanumeric strings, or, more fundamentally, strings of bits that, when evaluated by the algorithm, convert plaintext into ciphertext and vice versa.

A rudimentary (and easily reverse-engineered) encryption algorithm might convert each letter of plaintext into a letter of ciphertext by first assigning a numeric value to each letter of the alphabet, then adding to the plaintext character's numerical value the number provided by the key, and then converting the value back to a letter. If, for example, the key is "3," each "A" would become a "D," each "J" would become an "M," each "Z" would become a "C," and so on. (Algorithms, of course, get more complicated, but the basic concepts remain the same.) The algorithm is the lock, and only the keys that fit will open it, revealing the locked container's contents.

In digital cryptography, encryption algorithms, or ciphers, are so complex that only computers can encrypt and decrypt data. Keys likewise are long enough to make it difficult, if not impossible, to try every possible key combination in an effort to circumvent the encryption. Indeed, encryption algorithms can be, and often are publicly known and understood without compromising the security of information encrypted using them.

There are two types of keys: symmetric and asymmetric. Symmetric keys can be used both to encrypt and decrypt the same content. The example key above is a symmetric key: to encrypt, the "3" is added to the letter's numeric value; to decrypt, it is subtracted. For symmetric keys to work, the sender and receiver of the secure information must have the key, which means they must arrange beforehand to share it with each other.

Symmetric keys become less useful at a large scale. For example, in order for any two individuals to communicate securely, they each would need the same symmetric key, and they would have had to exchange it in a secure manner prior to communicating. If a third person joins the group, and each of the original two desires to communicate with the third without the other eavesdropping, each pair of potential communicators would need a unique symmetric key. In a group of three people, there are three unique pairs. In a group of five, there are ten. In a group of ten thousand, there are 49,950,000.

Since users may want to communicate with other users prior to actually meeting them and exchanging a symmetric key, a central trusted authority, often a server, is required to pool the keys and distribute them to the users using a scheme sometimes called a Kerberos system. This creates a key distribution problem, though: the management of all the keys necessary to maintain a large network with a constantly changing composition is unwieldy and unreliable, as it depends entirely on the availability of the central server and the ability of that server to know who in the network desires access to others. In a corporate network, that task might be manageable; on the scale of the entire Internet, it is practically impossible. In addition, symmetric key schemes become more complicated when users desire to communicate with multiple users at once. Finally, the reliability and integrity of the scheme relies entirely on the reliability and integrity of the Kerberos server. If the server is compromised, the system breaks down.

Asymmetric keys are one way to solve the key distribution problem. Asymmetric keys either encrypt or decrypt, which means that two asymmetric keys are required for any one transmission: one to encrypt and a second to decrypt. One use of asymmetric keys is in public-private encryptions schemes, which are akin to conventional mailboxes. The public key corresponds to an address; the private, to the mailbox key. Anyone with the recipient's public key can encrypt a message for the recipient, but the message cannot be decrypted with that key, just as a member of the public cannot access mail already delivered through a locked mail slot, even if they know the recipient's address. Instead, only the recipient can decrypt the message, by using the private key that only the recipient has, just as the mail recipient uses a key to open the mailbox and retrieve the mail.

A similar asymmetric key scheme is a digital signature system, whereby a sender's private key is used to generate a signature, which accompanies the transmission. The signature can only be verified by using that sender's public key, not unlike authentication of a letter via a wax seal. If, after the public key is applied to the algorithm, the signature does not compute correctly, the recipient knows the identity of the sender, or the integrity of the transmission itself, cannot be verified.

Although public-private key schemes obviate the need for sender and recipient to meet

United States District Court
Northern District of California

beforehand to exchange a key, they introduce another problem: the integrity of the message can be compromised if the public key does not actually correspond to its intended owner, but rather to a bad actor that has intercepted the communication and, by distributing a different public key, has surreptitiously convinced the user that it is the intended recipient of the communication. The solution, known as public-key infrastructure ("PKI"), involves the use of independent third parties, known as certificate authorities, who can certify the authenticity of public keys. As long as the third party certificate authority authenticates the public key in a satisfactory manner, *i.e.* in person, or otherwise offline in a manner that sets aside any legitimate question of authenticity, and, as long as the certificate authority retains the public's trust, PKI remains workable. In fact, the public keys for the most popular Internet servers are distributed with Internet browsers, or with an operating system, making the process even simpler. PKI is commonly used to secure online banking, online shopping, and other highly sensitive online activities.

Encryption schemes are usually used in combination with one another to establish secure transmissions and send and receive secure communications. For example, an internet server and a computer user may first utilize a public-private key scheme to establish a private access line ("PAL"), after which messages may be sent back and forth securely with confidence that the sender and recipient are who they say they are. Further, once the PAL is established, the internet server may send the user encrypted content, such as a video stream, that the user may only decrypt by using the appropriate key, depending on whether the user is authorized to view the content. One way for the server to make the determination is to distribute a symmetric key that corresponds to the video stream. But then anyone could share the key with unauthorized users, who could then view the stream, too.

Another method could involve public-private key encryption, whereby the internet server uses the public key for each intended viewer to encrypt the stream, and the viewer decrypts the stream using the viewer's private key. The weakness of that approach is that the server must encrypt the symmetric key that decrypts the stream separately for each intended viewer, and either send the stream individually for each user, or send it all as one package of encrypted symmetric keys, forcing the user either to look for the right public key among the encrypted symmetric keys, or to refer to a list of users who have access to determine which encryption is the right one, which means the access list is public to anyone who downloads the file.

B. Patents-in-Suit

The two patents-in-suit, U.S. Patents 7,257,706 ("the '706 patent'") and 7,743,249 ("the '249 patent'") are both titled "Method of Securing a Document in a System and Controlling Access to the Document and a Seal for Use in the Method." They are the final two patents in a series of five patents assigned to TriStrata concerning the security of computer documents: U.S. Patents 5,960,086 ("'086 patent") (Atalla, 1995); 6,088,449 ("'449 patent") (Atalla, 1996); 6,912,655 ("'655 patent") (Zucker, 1999); the '706 patent (Zucker, Atalla, Adams, 2005); and the '249 patent (Zucker, Atalla, Adams, 2007). The last three patents share a common specification, as each is a continuation of the last.[1] Each patent also incorporates the earlier patents in the series by reference. Finally, the 1999 patent also incorporates abandoned patent application number 09/095,350. The patents-in-suit are directed at the problems associated with broadcast (one-to-all) and multicast (one-to-many) transmissions described above. In particular, the '706 and '249 patents claim a "method for efficient multicast key management." '706 patent, col. 2:22–23; '249 patent, col. 2:25–26.

II. LEGAL STANDARD

The construction of terms found in patent claims is a question of law to be determined by the court. Markman v. Westview Instruments, Inc., 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc), aff'd, 517 U.S. 370 (1996). "[T]he interpretation to be given a term can only be determined and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim." Phillips v. AWH Corp., 415 F.3d 1303, 1316 (Fed. Cir. 2005) (quoting Renishaw PLC v. Marposs Societa' per Azioni, 158 F.3d 1243, 1250 (Fed. Cir. 1998)). Consequently, courts construe claims in the manner that "most naturally aligns with the patent's description of the invention." Id.

The first step in claim construction is to look to the language of the claims themselves. "It

[1] Because they share a specification, the Court will focus on the '706 patent where appropriate.

is a 'bedrock principle' of patent law that 'the claims of a patent define the invention to which the patentee is entitled the right to exclude.'" Phillips, 415 F.3d at 1312 (quoting Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc., 381 F.3d 1111, 1115 (Fed. Cir. 2004)). A disputed claim term should be construed in light of its "ordinary and customary meaning," which is "the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." Phillips, 415 F.3d at 1312. In some cases, the ordinary meaning of a disputed term to a person of skill in the art is readily apparent, and claim construction involves "little more than the application of the widely accepted meaning of commonly understood words." Id., at 1314. Claim construction may deviate from the ordinary and customary meaning of a disputed term only if (1) a patentee sets out a definition and acts as his own lexicographer, or (2) the patentee disavows the full scope of a claim term either in the specification or during prosecution. Thorner v. Sony Computer Entm't Am. LLC, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

Ordinary and customary meaning is not the same as a dictionary definition. "Properly viewed, the 'ordinary meaning' of a claim term is its meaning to the ordinary artisan after reading the entire patent. Yet heavy reliance on the dictionary divorced from the intrinsic evidence risks transforming the meaning of the claim term to the artisan into the meaning of the term in the abstract, out of its particular context, which is the specification." Id., at 1321. Typically, the specification "is the single best guide to the meaning of a disputed term." Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576, 1582 (Fed. Cir. 1996). It is therefore "entirely appropriate for a court, when conducting claim construction, to rely heavily on the written description for guidance as to the meaning of claims." Phillips, 415 F.3d at 1315. However, while the specification may describe a preferred embodiment, the claims are not necessarily limited only to that embodiment. Id.

Finally, courts may consider extrinsic evidence in construing claims, such as "expert and inventor testimony, dictionaries, and learned treatises." Markman, 52 F.3d at 980. Expert testimony may be useful to "provide background on the technology at issue, to explain how an invention works, to ensure that the court's understanding of the technical aspects of the patent is consistent with that of a person of skill in the art, or to establish that a particular term in the patent or the prior art has a particular meaning in the pertinent field." Phillips, 415 F.3d at 1318. However, extrinsic evidence is "less reliable than the patent and its prosecution history in determining how to read claim terms." Id. If intrinsic evidence mandates the definition of a term that is at odds with extrinsic evidence, courts must defer to the definition supplied by the former. Id.

III. CLAIM TERM CONSTRUCTIONS

The '706 and '249 patents are directed at an "efficient multicast key management" scheme that "is achieved by using seals." '706 patent, abs.; '249 patent, abs. Four of the patents in the five-patent series use the term "seals." Nothing in any of the five patents explicitly defines the term despite its central role in the patent claims.

The specification shared by the patents-in-suit teaches that secure broadcast and multicast transmissions are difficult to accomplish by using (1) conventional, or symmetric, encryption, or (2) PKI cryptography. The former is unwieldy and insecure; the latter leads to the multicast key management problems discussed above. See '706 patent, col. 1:23–2:16. As in symmetric encryption, the distribution and maintenance of encryption keys in PKI cryptography in a broadcast context becomes "difficult and impractical." Id. 2:16.

The summary of invention discloses a system that involves "the transmission of what are called 'permits' and 'seals' to allow the storage of secured documents and the accessing of secured documents by authorized clients or for secured messaging between clients." Id. 2:26–30. "[T]he security server generates what is called a 'seal.'" The "seal" may contain a key or information to generate a key. Id. 2:32–35. "The security server encodes this key or information to generate this key using any encryption method. The encoded key is called a 'seal' which is generated by the security server." Id. 2:35–36. The seal may also contain a user identification code, "a policy which is a description as to who is allowed access to what," a message digest made up of a hash of files, or a date and time stamp. Id. 2:32–45. "The key or the information to generate the key is often called a 'permit,' so the permit is contained within the seal but may not be the exclusive contents of the seal." "All the information contained in a seal is encrypted by the security server and can only be 'opened,' i.e., decrypted, by the security server which encrypted the seal." Id. 2:46–49.

The broadcast transmission scheme disclosed by the patents includes three sets of actors: security servers, application servers, and application clients. The latter two may be, for example, a web server and a web user, or a database and a database client. Id. 2:53–56. The application server requests a seal from the security server. The security server returns one, and the application server "then broadcasts the seal to a plurality of application clients. Each client wishing to encrypt or decrypt a data stream sends the seal it received from the application server to the security server in an open seal request signal, together with the client's identification information, so that the seal can be 'opened.'" Id. 2:59–66. The security server "decrypts the seal and compares the client's identification with the policy stored at the security server." Id. 2:57–3:1. If the policy provides for access by the client, the security server "extracts a permit from the decrypted seal and transmits the permit to the client in clear text form." Id. 3:2–4. The client can then use the permit to encrypt or decrypt the data stream. In this manner, the patents "solve[] the broadcast key distribution problem." Id. 7:64–65.

The parties dispute the proper construction of a number of claim terms, most important of which is the parties' dispute over the meaning of the term "seal."

C. "seal"

Claim Term	TriStrata's Proposed Construction	Microsoft's and Adobe's Proposed Construction
"seal" All claims	Information in the form of computer bits used by a computer system to secure documents through encryption. The seal contains information relating to an encryption/decryption key, such as information from which the key can be derived or the key itself.	An encrypted data structure generated by a security server and containing a key or information to generate a key, wherein the entire data structure is symmetrically encrypted and decrypted only by the security server that created it.

i. Intrinsic Evidence

In construing disputed claim terms, the Court first looks to the language of the claims themselves. The term "seal" appears in most of the '706 and '249 patents' claims. Relevant recitations include:

'706 Patent

> **Claim 1:** A method of securing a document stored in a computer system which is part of a network, comprising:
>
> creating a seal associated with a document which is to be stored or shared within the computer system or network:
>
> placing in the seal information identifying the person requesting that the document be secured (hereinafter the "requestor"); and
>
> placing in the seal information identifying who can access the document;
>
> thereby allowing one or more designated persons to have access to the document in accordance with the information in the seal.
>
> **Dependent Claim 2:** The method as in claim 1 wherein said seal includes a unique key.
>
> **Dependent Claim 3**: The method of claim 2 further comprising sending said key to the requestor so that the key can be used by the requestor to encrypt the document.
>
> * * *
>
> **Claim 14:** A method for sealing and controlling access to a document stored or communicated in a computer system which is part of a network which comprises:
>
> creating a seal as part of a document which remains a part of the document when the document is in storage or when the document is sent in communication or is shared anywhere within the computer system or network; and
>
> encrypting said seal using a unique key at a server:
>
> said seal allowing the system to validate the requestor, and identify those authorized by the requestor to have access to the document.
>
> * * *
>
> **Claim 28**: A seal for sealing and controlling access to a document stored or communicated in a system which is part of a network, said seal comprising selected information . . . wherein said seal is encrypted using a unique key at a server . . . ."

'249 Patent

> **Claim 1:** A system for securing a document stored in a computer system which is part of a network, comprising:
>
> a storage device storing a seal for association with a document which is to be stored or shared within the computer system or network, said seal comprising;

> a) information identifying a requestor requesting that the document be secured; and
>
> b) information identifying one or more parties qualified to access the document.

Because the patents-in-suit are continuations of the ’665 patent, and because they incorporate by reference the ’449 patent, those patents’ claims and specifications are also relevant intrinsic evidence. See In re Katz Interactive Call Processing Patent Litig., 639 F.3d 1303, 1325 (Fed. Cir. 2011) (“[W]e ordinarily interpret claims consistently across patents having the same specification. . . .”); Cook Biotech Inc. v. Acell, Inc., 460 F.3d 1365, 1377 (Fed. Cir. 2006) (reference to same claim term in prior art “was intended to refer to the same structures” where later patent incorporated prior art by reference).

The term “seal” first appears in the ’449 patent, the second of the five patents in the series, which claims a method of securing the transmission of information through a key management scheme that involves digital signatures. The specification first uses the term “seals” in the context of a particular embodiment as follows: “The server will establish a private access line (“PAL”) which provides I.D. and authentication between the client and the security server. The system allows the transmission of what is called permits and seals to allow the storage of secured documents and the accessing of secured documents by authorized clients or for secured messaging between clients.” ’449 patent, col. 9:58–64. That patent does not contain a definition of the term, though claim 17, which recites a method of encrypting information through the use of “pointers,” or data that points to specific byte addresses, refers to the term “seal” as collectively referring to two encrypted pointers, which are transmitted along with the document.

The ’655 patent, titled “Network Security Architecture System Utilizing Seals,” contains the same specification as those in the patents-in-suit. In addition to the use of the term “seal” in that specification, independent claim 6 recites “[a] method of key management, comprising: generating a set of encrypted seal bits at a security server; transmitting said set of encrypted bits” from the security server to an application server, and several other steps. Independent claim 11 recites “[a] method for opening a seal, wherein said seal comprises a set of encrypted bits comprising information for generating a set of encryption/decryption bits.”

ii. Ordinary and Customary Meaning

The Court must construe disputed claim terms as having "the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention." Phillips, 415 F.3d at 1312. Ordinary and customary meaning can only be ascertained "after reading the entire patent. It is the specification that serves as "the single best guide to the meaning of a disputed term." Vitronics, 90 F.3d at 1582.

Claim construction is not an exercise conducted in a vacuum, "but in the context of the entire patent, including the specification." Phillips, 415 F.3d at 1313. Thus, even where terms do not, standing alone, have a customary meaning in the art, if a person of ordinary skill in the art could derive the term's meaning after reading the entire patent, then the ordinary meaning, as interpreted by the person of ordinary skill, controls. See Honeywell Int'l Inc. v. Universal Avionics Sys. Corp., 488 F.3d 982, 990 (Fed. Cir. 2007) (where claim terms had no ordinary meaning to a skilled artisan, patent provided necessary context to define the term) (citing Irdeto Access., Inc. v. Echostar Satellite Corp., 383 F.3d 1295, 1300 (Fed. Cir. 2004)).

Here, the parties agree that the term "seal" had no ordinary and customary meaning in the art at the time of invention. See Wecker Decl. ISO TriStrata's Claim Constructions, ECF No. 59, Ex. 11 at 193:14–21 (July 13, 2013 Deposition of Donald Adams) ("We took the name 'seal' from the old wax seal that was put on physical objects."); Wesenberg Decl. ISO Microsoft's Claim Constructions, ECF No. 66-1, Ex. A p. 13 (Mazières Expert Report); id., Ex. B ¶ 22 (Rubin Expert Report); Belloli Decl. ISO Adobe's Claim Constructions, ECF No. 65, Ex. C ¶ 22 (Rubin Expert Report).

TriStrata argues that its construction is consistent with the ordinary meaning of "seal" as derived from a general-purpose dictionary, i.e., "something that secures (as a wax seal on a document)." TriStrata maintains that the intrinsic evidence demonstrates "nothing was intended to be conveyed by the term ["seal"] other than the common sense meaning of something that protects a message." ECF No. 58 p.8. Tristrata's reliance upon a dictionary definition is problematic, however, for a number of reasons.

First, Tristrata's proposed construction is much narrower than the broad dictionary definition, "something that secures." It is not clear that one follows from the other.

Second, even if general-purpose dictionaries supported Tristrata's construction, the Federal Circuit has rejected the use of dictionary definitions without regard to the language of the patent. "[H]eavy reliance on the dictionary divorced from the intrinsic evidence risks transforming the meaning of the claim term to the artisan into the meaning of the term in the abstract, out of its particular context, which is the specification." Phillips, 415 F.3d at 1321. Thus, the Phillips court held, claim terms must be construed in light of and only after reading the entire patent. Indeed, "in the absence of something in the written description and/or prosecution history to provide explicit or implicit notice to the public — i.e., those of ordinary skill in the art — that the inventor intended a disputed term to cover more than the ordinary and customary meaning revealed by the context of the intrinsic record, it is improper to read the term to encompass a broader definition simply because it may be found in a dictionary, treatise, or other extrinsic source." Nystrom v. TREX Co., Inc., 424 F.3d 1136, 1145 (Fed. Cir. 2005).

Defendants, relying on Irdeto, 383 F.3d at 1300, argue that disputed terms that lack customary meaning in the art must be construed "only as broadly as provided for by the patent itself." The patentee's failure expressly to define the term "seal," argue Defendants, merits a departure from the "heavy presumption" in favor of construing claim terms according to their ordinary meaning.

The patentee in Irdeto claimed "a system for controlling the broadcast of digital information signals by using three layers or tiers of complementary encryption and decryption keys." Id. at 1296. The specification of the patent-in-suit consistently used the term "group," in the phrase "group key," to refer to a subset of all subscribers of the satellite television service. The plaintiff asserted that the term applied to a group of *all* subscribers, based on the ordinary meaning of the term "group." The Federal Circuit held that the specification limited the ordinary meaning by the repeated and consistent implication that "group keys" are keys shared by a subset of subscribers.[2] The Irdeto court also noted that "where evidence such as expert testimony or

[2] Also relevant to the Federal Circuit's decision in Irdeto, and absent in this case, was the applicant's communication with the patent office demonstrating an intent to act as a lexicographer

technical dictionaries demonstrates that artisans would attach a special meaning to a claim term or would attach no meaning at all to the claim term independent of the specification, 'general-usage dictionaries are rendered irrelevant with respect to that term . . . .'" Id. at 1300 (quoting Vanderlande Indus. Nederland BV v. Int'l Trade Comm'n, 366 F.3d 1311, 1321 (Fed. Cir. 2004)).

Here, the term "seal" has a plain English meaning. The parties agree that the term was not customarily used in the art, but rather was adapted by the inventor for use in cryptography as a metaphor for physical, wax seals. A person of ordinary skill, after reading the entire patent, would understand, first, that the term is used in the claims and the shared specification as an analog for wax seals, but in a manner that has been adapted to fit the needs of the claimed invention. The plain and ordinary meaning of the term "seal" that a skilled artisan would derive from the patent specification has certain, specific limitations: namely, (1) the seal must be an encrypted data structure, (2) it must contain a key or information to generate a key, and (3) it must be encrypted by a security server, and capable of decryption only by the server that generated it. Those limitations are evident from the patents themselves, and they are essential to the term as it is used in the patents' claims.

iii. Limitations

a. Encrypted Data Structure

The claims themselves provide no definitions, or even context from which a definition can be derived, of the term "seal." They do clarify that a seal will, at a minimum, contain two pieces of information: the identity of the requestor, and information identifying who can access the document. However, the summary of the invention makes clear that a seal, as disclosed by the patents-in-suit, is an encrypted data structure. Where the specification discloses non-exclusive embodiments, it uses the phrase "In one embodiment," or "In another embodiment." By contrast,

in the first instance. Id. ("[The] applicant informed the examiner and all competitors that the "key" modifiers — 'service,' 'group,' and 'box' — have no accepted meaning in the art and 'are very adequately described in the specification.' The applicant's use of those terms in the specification thus controls their scope."). However, the Irdeto court's decision did not rest on that factor, as it found that the patent's context defined the term even absent the express disavowal normally required for Thorner redefinition.

in discussing the security server/application server/application client scheme described above, the specification contains no such disclaimers. Instead, the entire scheme is described following the preface: "In accordance with this invention, ..." '706 patent, col. 2:50.

The patents claim a method whereby the seal is unreadable, and unusable, by anyone but the security server that created it. The specification repeatedly teaches that security servers "open" seals, unpack their contents, and return to the user the appropriate information or data. See id. 2:65, 3:20. "All the information contained in a seal is encrypted by the security server and can only be 'opened,' i.e. decrypted by the security server that encrypted the seal." Id. 2:46–49. If the seal were not encrypted, the security scheme would not function, and the security server would serve no purpose, as it would be transmitted in plaintext. Indeed, the claims themselves, which recite methods of securing documents, contain nothing other than the term 'seal' that relates to the actual encryption of a document.

TriStrata argues that every limitation identified by Defendants is derived from a non-limiting embodiment. For example, TriStrata argues that one of the paragraphs discussing the encryption of seals also contains the phrase "In one embodiment," see id. 2:31–49, rendering the remainder of the paragraph non-limiting. A plain reading of the paragraph yields the opposite conclusion: though it discloses three embodiments, it also teaches that, in any embodiment, the contents of the seal are encrypted by the security server and can only be opened by it.

TriStrata also argues that even if the keys contained in the seal must be encrypted, other pieces of information in the seal need not be encrypted, and suggests that, at most, the seal must be partially, but not necessarily completely encrypted. The Court agrees. Indeed, the patent discusses several types of information that may be contained in a seal, some of which, such as permits, must be encrypted, and others of which, such as date and time stamps, need not be. In addition, the patent specifically provides for the encryption of seals by security servers "using any encryption method," not just symmetrical encryption. Id. 2:35–36. Defendants' proposed construction must therefore be amended to read: "A data structure generated by a security server and containing a key or information to generate a key, wherein part or all of the data structure is encrypted and decrypted only by the security server that created it."

b. Contains a Key, or Information to Generate a Key

The seal contains a key, or information that can be used to generate a key. TriStrata disputes this limitation even though its own proposed construction includes: "The seal contains information relating to an encryption/decryption key, such as information from which the key can be derived or the key itself." TriStrata does not explain what, if any other types of information other than the key itself and information used to generate it may be contained in a seal. Instead, Plaintiff argues that nothing disclaims "other embodiments that may be devised to allow the seal of the Patents to accomplish its purpose of protecting documents." ECF No. 58 p. 15. That argument is not persuasive. The limitation as proposed by Defendants adequately encompasses the broadest possible scope disclosed by the specification.

c. Generation, Encryption, and Decryption by Security Server

For the same reasons that seals must be encrypted data structures, they must be generated by a security server, encrypted by the security server, and decrypted by the same security server. The patents disclose that precise method in general terms, not as non-limiting embodiments. Nothing in the patents suggests that seals could be generated in another way, or that they could be encrypted by one entity and decrypted by another. The specification specifically forecloses that possibility: "All the information contained in a seal is encrypted by the security server and can only be 'opened,' i.e., decrypted, by the security server which encrypted the seal." '706 patent, col. 2:46–49.

iv. TriStrata's Motion to Supplement the Record on Claim Construction

After the claim construction hearing, TriStrata moved to supplement the record on claim construction with a document Microsoft produced in discovery after the hearing occurred. ECF No. 123. Microsoft opposed the request on procedural and substantive grounds. The Motion is hereby GRANTED.

However, having reviewed the document, the Court concludes that it does not alter the Court's claim construction analysis. The document is Microsoft's MS Digital Asset Server Digital Rights Management Specification for eBooks ("DAS specification"). It concerns unrelated, proprietary Microsoft technology. The document defines the term "Seal/Unseal" in the context of eBooks as: "Act of exposing or hiding Symmetric Keys required to encrypt/decrypt and use protected eBooks." "Sealed eBooks" are defined as: "Encrypted during the conversion to the .lit file. It ensures the authenticity of content, meaning that the text and other content cannot be modified. . . ." A "Sealed Copy" is defined as "An eBook that has been encrypted with a Symmetric Key, which has been itself encrypted with a cryptographic hash of the metadata in the title. . . ."

TriStrata makes two conflicting arguments about the DAS specification. First, TriStrata argues that the document uses the word "seal" in a way that "clearly evok[es] the meanings [of] the term as defined in the general purpose dictionaries." ECF No. 123 at 2. Second, TriStrata argues the document "clearly demonstrates that skilled artisans around the time of the patent application used the term in the very fashion that TriStrata has [has] claimed." ECF No. 126 at 1.

The Court is not persuaded by either contention. With regard to TriStrata's "dictionary definition" argument, the Court has concluded that the patentee did not intend to use the term "seal" in the same way that the term is defined in a general purpose dictionary. Moreover, even TriStrata's proposed construction of the term is not consistent with a general purpose dictionary definition. Rather, an appropriate construction is one that relies on the language of the specification. Nothing in the Microsoft document changes that fact; in fact, the DAS specification does not use the term "seal" in accordance with the general purpose dictionary definition, either.

With regard to TriStrata's second argument, the Court notes that the definitions in the DAS specification themselves contain limitations that are either inapposite here, or that are inconsistent with TriStrata's proposed construction. For example, "Seal" is defined as the act of hiding a symmetric key. A "Sealed eBook" must be encrypted with a symmetric key, and then encrypted again using the cryptographic hash from metadata, while TriStrata argues that a seal need not be completely encrypted at all, and argues against the limitation of the term "seal" as requiring symmetric encryption. And eBooks themselves appear in each definition, which are obviously unrelated to the patents-in-suit. In short, the DAS specification document is not helpful to the Court.

For the foregoing reasons, the Court therefore construes the term "seal" as: "A data structure generated by a security server and containing a key or information to generate a key, wherein part or all of the data structure is encrypted and decrypted only by the security server that created it."

D. "key"

Claim Term	TriStrata's Proposed Construction	Microsoft's and Adobe's Proposed Construction
"key" '706 patent, claims 2, 3, 4, 11, 14, 17, 18, 25, 28 '249 patent, claims 2, 3, 4	Cryptographic string of computer bits used in an encryption/ decryption process to make data unreadable without access to the key.	A secret string of bits with which a message can be encrypted and subsequently decrypted.

Unlike the term "seal," the term "key" unquestionably has an ordinary and customary meaning in the art, which is accurately captured by TriStrata's proposed construction. As described above, keys can be symmetric or asymmetric. Nothing in the claims, the patents, or extrinsic evidence suggests that the patentee acted as his own lexicographer in using the term "key." To the contrary, the term is used frequently throughout the patents, which themselves explain the difference between symmetric and asymmetric keys.

Defendants' proposed construction seeks to limit the term to symmetric keys that are secret. Nothing in the claims themselves supports that position, nor does a full reading of the patents suggest that, each time the patentee used the term "key" in the patent claims, the patentee intended to limit the term to symmetric keys, even though throughout the specification and prior art the term is used to mean one or both of symmetric and asymmetric keys.

The Court agrees, however, that TriStrata's construction is unnecessarily confusing, as it suggests that decryption can make data unreadable. In addition, it fails to account for the difference, if there is any, between a "cryptographic" string of bits and an ordinary string of bits. The Court therefore construes the term "key" as follows: "A string of bits used in encryption to make data unreadable, or in decryption to render encrypted data readable."

E. "encrypt"

United States District Court
Northern District of California

Claim Term	TriStrata's Proposed Construction	Microsoft's and Adobe's Proposed Construction
"encrypt" '706 patent, claims 14, 28	Disguise a message in such a way as to hide its substance from someone not permitted to have access to the message.	Use a key to disguise a message in such a way as to hide its substance from those who do not know the key.

The parties' proposed constructions of "encrypt" are virtually identical, but each suffers from a significant flaw. TriStrata's proposed construction fails to account for the possibility that someone not permitted to have access to the message may nevertheless be able to read it by obtaining unauthorized access to a method of decrypting it. Defendants' construction limits encryption to symmetric encryption, which limitation is not supported by the patent. Otherwise, the parties appear to agree that encryption is the process of disguising information from those who do not have the key necessary to decrypt it. The Court therefore construes the term "encrypt" as follows: "To disguise information such that it is unreadable to anyone who does not have the key necessary to decrypt it."

F. "information identifying who can access the document" and "information identifying who can/one or more parties qualified to access the document"

Claim Term	TriStrata's Proposed Construction	Microsoft's and Adobe's Proposed Construction
"information identifying who can access the document" "information identifying who can/one or more parties qualified to access the document" '706 patent, claims 1, 6, 16, 20, 25, 28 '249 patent, claims 1, 7	Information that identifies one or more persons who are permitted to have access to the document.	Plain and ordinary meaning in view of the intrinsic record and knowledge of one of ordinary skill.

The parties disagree as to the scope of the terms "information identifying who can access the document," as found in the '706 patent, and "information identifying who can access the document," and "information identifying one or more parties qualified to access the document," as found in the '249 patent. TriStrata seeks to exclude from the terms information identifying categories or classes of people, as opposed to information identifying specific users. TriStrata does not identify anything in the patents to support its proposed limitation. Nothing in the patents limit the concept to the identification of individuals rather than individuals who are part of larger groups. Indeed, the '706 patent twice, in nearly identical language, explains that "[t]he policy … is a description as to *who is allowed access* to what (*e.g., classification of files and security levels of clients*), which is consistent with information identifying categories or classes of users." '706 patent, col. 2:39–41, 6:65–67 (emphasis added).

The Court agrees with Defendants that a plain meaning construction is appropriate. A person of ordinary skill in the art would understand the meaning of the disputed terms, and would also understand that they may apply to information identifying classes of people, or individual people, depending on the application.

G. "information which allows the computer system to confirm server identity"

Claim Term	TriStrata's Proposed Construction	Microsoft's and Adobe's Proposed Construction
"information which allows the computer system to confirm server identity" '706 patent, claims 13, 27 '249 patent, claim 13	Information that allows the computer system to verify server identity information.	Pointers that are exchanged to establish the private access line that provides authentication and identification between the client and the security server.

Defendants propose to import several limitations into the term "information which allows the computer system to confirm server identity" as it appears in the '706 and '249 patents, based on one embodiment discussed in the specification of the '706 patent. See '706 Patent, col. 5:51–54. The patents-in-suit do not define the term, and nothing in the patent suggests that the patentee intended to limit the term to the embodiment Defendants rely upon. Indeed, the beginning of the subject paragraph disclaims any such limitation. See id. 5:44 ("In one embodiment of the '449 patent . . ."). Moreover, as Plaintiff argues, U.S. Patent Application No. 09/095,350, an abandoned application incorporated by reference into the specifications of the patents-in-suit, describes a different method for confirming server identity. See U.S. Patent Application No. 09/095,350, Wecker Decl. ISO Pl.'s Opening Claim Construction Brief, ECF No. 59, Ex. 8, pp. 14:22–16:13 (describing method for authenticating server and sender identities).

The Court adopts Tristrata's construction of this term: "Information that allows the computer system to verify server identity information."

H. Means Plus Function Claims

The parties dispute whether claim 4 of the '249 patent is indefinite.[3]

When claims use the term "means" to describe a limitation, they are presumed to be means-plus-function limitations. Altiris, Inc. v. Symantec Corp., 318 F.3d 1363, 1375 (Fed. Cir. 2003). See 35 U.S.C. § 112 ¶ 6. Claim 4 recites: "The system of claim 3 further including means for allowing the requestor to discard the key following the encryption of the document." TriStrata concedes that claim 4 is a means-plus-function claim. In construing such claims, "(1) the court must first identify the function of the limitation; and (2) the court must then look to the specification and identify the corresponding structure for that function." Biomedino, LLC v. Waters Technologies Corp., 490 F.3d 946, 950 (Fed. Cir. 2007). "[I]n order for a means-plus-function claim to be valid under § 112, the corresponding structure of the limitation must be disclosed in the written description in such a manner that one skilled in the art will know and understand what structure corresponds to the means limitation. Otherwise, one does not know what the claim means." Id. If the patent does not disclose structure corresponding to the means-plus-function limitation, the system claim is invalid as indefinite. Id.

Defendants argue that claim 4 is invalid as indefinite pursuant to 35 U.S.C. § 112 ¶ 2, for failure to disclose a structure corresponding to the claimed function. TriStrata argues that the '086 patent, incorporated by reference by the '249 patent, discloses sufficient structure because it

[3] TriStrata concedes Adobe's proposed identifications of structure pertaining to claims 3, 5, and 6 of the '249 patent. ECF No. 70 p. 14.

explains that keys are used only once. The ’249 patent likewise discloses a method for encryption of a data stream with a key “to be used only once and then changed in a manner which is essentially random.” ’249 patent, col. 4:61–64. That disclosure refers to the’086 patent.

TriStrata has not adequately identified a structure that corresponds to claim 4. Although the ’249 and ’086 patents disclose methods that involve using keys only once, they do not disclose any structure for discarding the keys; they merely state that the keys are discarded. The Court therefore finds that claim 4 is invalid as indefinite.

IV. MOTION TO STRIKE TRISTRATA’S TECHNOLOGY TUTORIAL

Following the Court’s denial without prejudice of Defendants’ *ex parte* motion to strike portions of TriStrata’s technology tutorial, ECF No. 95, Defendants renewed their motion to strike, and requested that the Court disregard pages 4, 5, 7, 8, 10, 12, 13, 15–17, and 28–30 of TriStrata’s technology tutorial presentation, ECF No. 100 (Mot.), on the grounds that those pages contain impermissible argument and violate this Court’s Order prohibiting TriStrata from presenting the stricken expert testimony contained in the late-filed declaration of David Bernstein, ECF No. 87 p. 5.

“[T]rial courts generally can hear expert testimony for background and education on the technology implicated by the presented claim construction issues, and trial courts have broad discretion in this regard.” Key Pharmaceuticals v. Hercon Laboratories Corp., 161 F.3d 709, 716 (Fed. Cir. 1998). See also, Markman, 52 F.3d at 980 (“The court may, in its discretion, receive extrinsic evidence in order ‘to aid the court in coming to a correct conclusion’ as to the ‘true meaning of the language employed’ in the patent.”) (quoting Seymour v. Osborne, 78 U.S. (11 Wall.) 516 (1871) (reviewing a decree in equity)). However, “if the meaning of a disputed claim term is clear from the intrinsic evidence — the written record — that meaning, and no other, must prevail; it cannot be altered or superseded by witness testimony or other external sources.” Id.

By agreement between the parties and order of the Court, the technology tutorial in question did not become part of the record. Indeed, the Court typically does not receive on-the-record technology tutorials, likely rendering any motion to strike portions of any tutorial moot. Because the tutorial is not part of the official record of the case, an order to “strike” it would not have any meaning. The motion is therefore denied.

For the same reason, the Court will deny Defendants' motion with respect to the oral presentation by expert witness David Bernstein at the parties' tutorial presentation. Defendants allege that Dr. Bernstein's comments contained material from his stricken Second Declaration, as well as improper argument concerning claim construction. Again, Dr. Bernstein's comments were not part of the record, and so there is nothing to "strike." At least as importantly, and as Defendants' motion itself makes clear, the Court was quite capable of separating the wheat of Dr. Bernstein's comments from the chaff without the need for post-hearing motion practice. See ECF No. 100 at 5 ("Indeed, Mr. Bernstein repeated this improper and tendentious assertion so many times that the Court asked him to desist").[4]

For these reasons, Defendants' Motion to Strike is DENIED.

V. CONCLUSION

For the foregoing reasons, the Court construes the disputed claim language as follows:

Claim	Term	Construction
all claims	"seal"	"A data structure generated by a security server and containing a key or information to generate a key, wherein part or all of the data structure is encrypted and decrypted only by the security server that created it."
'706 patent claims 2, 3, 4, 11, 14, 17, 18, 25, 28 '249 patent claims 2, 3, 4	"key"	"A string of bits used in encryption to make data unreadable, or in decryption to render encrypted data readable."

[4] The Court repeats this comment from Defendants' brief to demonstrate the lack of need for a motion, and not to adopt Defendants' verbiage.

United States District Court
Northern District of California

’706 patent, claims 14, 28	“encrypt”	“To disguise information such that it is unreadable to anyone who does not have the key necessary to decrypt it.”
’706 patent, claims 1, 6, 16, 20, 25, 28 ’249 patent, claims 1, 7	“information identifying who can access the document” “information identifying who can/one or more parties qualified to access the document”	Plain and ordinary meaning in view of the intrinsic record and knowledge of one of ordinary skill.
’706 patent, claims 13, 27 ’249 patent, claim 13	“information which allows the computer system to confirm server identity”	“Information that allows the computer system to verify server identity information.”

IT IS SO ORDERED.

Dated: October 15, 2013

JON S. TIGAR
United States District Judge